(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.[6]
G06F 9/44

(45) 공고일자 2001년09월29일
(11) 등록번호 10-0299954
(24) 등록일자 2001년06월13일

(21) 출원번호 10-1999-7002697
(22) 출원일자 1999년03월29일
(65) 공개번호 특2000-0048724
(43) 공개일자 2000년07월25일

(30) 우선권주장 08/724,176 1996년09월30일 미국(US)
(73) 특허권자 인텔 코오퍼레이션
미합중국 캘리포니아 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자 데이비스데렉엘
미국아리조나85044피닉스이스트데저트트럼펫로드4509
(74) 대리인 장용식, 박종혁

심사관 : 강갑연

(54) 안전 바이오스

명세서

기술분야

본 발명은 컴퓨터 펌웨어의 안전에 관한 것으로서, 보다 상세하게는, 개인용 컴퓨터('PC')와 같은 일반적인 컴퓨터 시스템에서 기본 입출력 시스템('BIOS'; 이하 바이오스)에 관한 것이다.

배경기술

컴퓨터 시스템에서 가장 중요한 소자중 한가지는 기본 입출력 시스템 ('BIOS')과 같은 부팅 펌웨어이다. 비휘발성 메모리의 일부 형태에서 전형적으로 저장되는 바이오스는 기계 코드이며, 중앙처리장치(CPU)가 초기화, 진단, 대량 기억장치로부터 운영 시스템 핵심을 로드하는 것, 및 루틴 입출력(I/O) 기능과 같은 작업을 수행할 수 있는 일반적으로 운영 시스템(OS)의 일부이다.

파워업후, BIOS에 상주하는 지시 코드를 인출함으로써 CPU는 부팅될 것이다. 고유 특성때문에, BIOS는 2개의 충돌되는 요구사항을 갖는다; (1) 수정되거나 파괴되면, 전체 시스템이 동작되지 않기 때문에 BIOS는 충분히 보호되어야한다. (2) BIOS는 소프트웨어 버그 또는 특성 향상을 위해 현장에서 업그레이드가 가능하도록 쉽게 수정가능해야한다.

전통적으로, BIOS는 소거 가능 피롬('EPROM')으로 실현된다. EPROM은 회로에서 수정되지 않는 장점을 갖는다. EPROM의 내용을 수정하기 위해서, 디바이스는 우선적으로 소켓으로부터 제거되고 자외선에 오랜 시간동안 노출됨으로써 소거되어야한다. 이러한 점에서, EPROM에서 실현된 BIOS는 바이러스 공격 그리고 전자 파괴행위에 대해 저항한다. 그러나, 이러한 디바이스는 회로내에서 프로그래밍이 가능하지 않기 때문에 EPROM 디바이스는 현장 업그레이드를 지원하지 않으며, 이것은 현장 업그레이드를 위해 필요한 특성이다. 현장 업그레이드로 인해 사용자는 비용이 드는 지연 및 부품 교환을 피하여 현장에서 BIOS를 업그레이드할 수 있다. 현장 업그레이드의 중요성때문에, 사실상 모든 BIOS 펌웨어는 이제 플래시 메모리를 사용하여 실현된다. 그러나, 현장에서 수정가능한 BIOS 플래시 메모리는, 금융 트랜잭션과 같은 민감한 응용에 파괴행위를 가져올 수 있는 바이러스 공격에 영향을 받기쉽다.

안전 보호가 없다면, BIOS 플래시 메모리로 실현된 종래의 컴퓨터 구조는 다양한 종류의 침입 공격에 영향을 받기 쉽다. 전형적인 바이러스 공격에서, 바이러스 코드는 코드 시퀀스를 실행하여 BIOS 플래시 메모리를 수정하려한다. 시스템이 다음번에 부팅되거나, 어떤 상태 또는 이벤트가 발생할 때, BIOS 플래시 메모리의 코드는 안전 보호가 없기에 파손되며 파괴 효과는 즉각적일 수 있다. 감염된 코드는 BIOS 코드 또는 운영 시스템 커널의 다른 영역으로 확장될 수 있다. 컴퓨터 시스템이 파워업될 때, BIOS는 수행될 제 1 프로그램이기때문에, 다른 시스템 또는 네트워크 바이러스 스캐닝 소프트웨어에 앞서, BIOS에 있는 바이러스의 검출 및 소거는 매우 어렵다. BIOS에 있는 바이러스는 스캐닝 소프트웨어로부터 자신의 흔적을 보이지 않게 효과적으로 숨길 수 있다.

따라서 본 발명의 주요 초점은 컴퓨터 바이러스에 의한 BIOS 파손을 방지하는데 있다. 이것은 BIOS 플래시 메모리의 내용이 수정되기전에 인증 및 유효성 검사를 개재함으로써 이루어진다.

본 발명에서 추구하는 접근방법은 암호화 코프로세서와 같은 인증 기능을 갖는 현존 하드웨어에 BIOS 플래시 메모리를 통합함으로써 BIOS 인증의 개념에 있다. 암호화 코프로세서는 BIOS를 기억하고 BIOS 갱신의 인증을 강화하기에, 공격자는 BIOS 내용을 파손시킬 방법을 갖지 못한다.

발명의 개요

본 발명은 실행가능한 코드를 안전하게 갱신하는 시스템을 설명한다. 시스템은, 코드 갱신을 기억하는 제 1 기억소자, 갱신될 필요가 있는 실행가능한 코드를 기억하는 제 2 기억소자, 제 1 기억소자와 코드 갱신을 식별하는 인증 코드, 및 안전 프로세서를 포함한다. 안전 프로세서는 디바이스 식별을 사용하여

코드 갱신 및 제 1 기억소자의 유효성을 검사하고 인증하기위해 제 2 기억소자에 연결된다.

도면의 간단한 설명

본 발명의 특성 및 이점은 본 발명의 다음에 따르는 상세한 설명에서 명백할 것이다.

도 1은 PCI 버스에 인터페이스될 수 있는 아호화 코프로세서 내부에 BIOS 플래시 메모리가 상주하는 본 발명의 도이다.

도 2는 호스트 프로세서에 의해 BIOS 프로그램에 대한 정상적인 판독 액세스동안 본 발명에서 발생하는 동작의 흐름도이다.

도 3은 BIOS 프로그램의 현장 업그레이드동안 본 발명에서 발생하는 동작의 흐름도이다.

발명의 상세한 설명

본 발명은 암호화 기술을 사용하여 BIOS 업그레이드와 같은 코드 갱신을 인증하고 유효성 검사하는 방법을 제공한다. 다음의 설명에서, 어떤 암호화 특성을 설명하기위해 일부 용어가 사용된다. 키는 리베스트, 샤미르 및 애들만('RSA'), 데이터 암호화 규격('DEA') 등에서 명시된 바와같은 데이터 암호화 알고리즘('DEA')과 같은 종래 암호화 알고리즘에 의해 사용되는 인코딩 그리고/또는 디코딩 파라미터이다. 증명은, 신용 기관(즉, 은행, 정부 기관, 기업등) 또는 제작자와 같은 다른 구성요소에 의해 유지되는 개인키에 의해 인코딩되며, 구성요소와 관련된 어떠한 디지털 정보(전형적으로 공개키)로서 정의된다. 디지털 서명은 인증과 유사하고, 인증 데이터를 위해 전형적으로 사용된다. 그리고, 안전이라는 용어는 침입자가 시스템에서 성공적으로 파손을 행하기에 계산적으로 수행불가능함을 의미한다. 안전 프로세서는 시스템에 안전 보호를 제공하기위해 안전 기능을 수행할 수 있는 전자 디바이스이다.

인증 및 유효성은 BIOS 펌웨어를 포함하는 안전 프로세서에 의해 수행된다. 이러한 안전 프로세서의 한 예는 암호화 코프로세서이다. BIOS 업그레이드에 매입된 디지털 서명과 같은 비밀 정보를 사용함으로써 암호화 프로세서는 BIOS를 인증하고 유효성을 검사한다.

도 1에서, 본 발명에서 실현된 컴퓨터 시스템의 실시예가 도시된다. 컴퓨터 시스템(10)은 호스트 프로세서(30), 시스템 메모리(32), 그리고 시스템 버스(33)에 연결된 디바이스사이에 통신을 지원하기위해 인터페이스로서 동작하는 칩셋(31)을 포함한다. 시스템 메모리(32)는 메모리 매핑된 I/O 디바이스뿐만 아니라 다양한 형태의 임의 접근 메모리('RAM'), 즉, DRAM, VRAM, SRAM 등과 같은 종래 메모리를 포함할 수 있으며, 상기 종래 메모리에 제한되지 않는다. 시스템 버스(33)는, 주변 구성요소 인터페이스('PCI'), 유니버설 시리얼 버스('USB') 등을 포함하는 어떠한 형태의 버스 구조에 맞춰 실현될 수 있다.

시스템 버스(33)에 연결될 수 있는 디바이스중 한 개는 암호화 코프로세서 (34)를 포함한다. 암호화 코프로세서(34)는 버스 인터페이스(40), 처리 유닛(41) 및 국부 비휘발성 메모리(42)를 포함한다. 시스템 버스(33)에 전기적 연결을 이루기위해 버스 인터페이스(40)가 사용된다. 처리 유닛(41)은 암호화 코프로세서(34)를 위한 주요 제어기로서 사용된다. 처리 유닛(41)은 자신의 고유 국부 비휘발성 메모리(42)와 인터페이스한다. 부팅 프로그램(43)은 비휘발성 메모리(42)내에 기억된다. 본 발명이 모호하지 않도록 필수소자만이 도시되었음을 이해할 것이다. 암호화 코프로세서(34)내에서 사용될 수 있는 필수적인 소자가 아닌 것은 RAM, 난수 생성기, 및 다양한 암호화 알고리즘 가속기를 포함한다. 게다가, 호스트 프로세서 (30)는 도 1의 암호화 코프로세서(34)로부터 분리되어 도시되지만, 암호화 코프로세서(34)는 호스트 프로세서(30)의 일부일 수 있으며 이때 호스트 프로세서 (30)는 시스템 버스(33)를 통해 가지않고 직접 BIOS 프로그램으로 액세스한다.

도 2에서, 시스템의 부팅과 관련된 단계가 도시된다. 우선, 단계(50)에서, 호스트 프로세서는 BIOS 프로그램에 상응하는 어드레스를 위해 판독 요구를 발생시킨다. 암호화 코프로세서는 관련된 BIOS 지시로 상기 요구에 응답한다(단계(60)). 마지막으로, 호스트 프로세서는 단계(70)에서 데이터를 처리한다. BIOS 지시를 계속 처리하기위해, 이 시퀀스가 반복된다.

전형적인 현장 BIOS 업그레이드에서, 소프트웨어 제작자(BIOS 벤더)는 사용자에게 새로운 BIOS 코드를 포함하는 디스켓을 보낼 것이며, 상기 코드는 업그레이드 동작을 수행하는 것이다. 사용자가 BIOS 업그레이드를 전자적으로 그리고 원격으로 다운로드할 수 있도록, BIOS 벤더가 공고 시스템, 또는 인터넷과 같은 데이터 초고속 연결을 확립하는 것이 또한 가능하다. BIOS 업그레이드에는 BIOS 플래시 메모리에 기록하고 소거하는 것이 필연적으로 관련된다.

도 3에서, BIOS 프로그램의 수정과 관련된 단계가 도시된다. 단계(110)에서, 호스트 프로세서는 대체 BIOS 명령을 암호화 코프로세서에 발생시킨다. 이 명령은 호스트 프로세서 자체에서 동작되거나 또는 원격 시스템에서 동작하는 일부 형태의 BIOS 관리 유틸리티 소프트웨어에 의해 전형적으로 생성된다. 이 명령의 목적은 새로운 BIOS 프로그램을 위한 암호화 코프로세서를 준비하는 것이다(단계(120)). 단계(130)에서, 암호화 코프로세서는 새로운 BIOS 프로그램 코드를 호스트 프로세서로부터 수동적으로 수신하거나 특정 소스(예를 들어, 시스템 메모리)로부터 새로운 BIOS 프로그램 코드를 능동적으로 검색한다. 단계(140)에서, 차후의 인증 동작이 특정한 새로운 BIOS 프로그램에서 수행되기위해 새로운 BIOS 프로그램은 내부적으로 보호된다. 단계(150)에서, 암호화 코프로세서는 새로운 BIOS 프로그램의 내부적으로 기억된 버전에서 적절한 인증 동작을 수행한다. BIOS 제공자 및 사용되는 암호화 코프로세서에게만 알려진 비밀정보를 사용하는 것을 포함하여, 인증이 수행될 수 있는 많은 방법이 있다. 인증 프로시저의 일부로서, 특히 새로운 BIOS 프로그램의 완전성 및 유효성을 검사하기위해 디지털 서명과 증명인 공지된 기술을 사용하여 공용/개인 키 암호화가 사용될 수 있다는 것이 이해될 것이다. 어떠한 인증 기술이 사용되든지, 새로운 BIOS 프로그램의 국부 버전에 대해 암호화 코프로세서내에서 인증 기술이 수행되는 것이 현저한 특징이다. 단계(160)에서 일단 인증 동작이 수행되었다면, 암호화 코프로세서는 새로운 BIOS

프로그램의 유효성으로서 특정할 수 있다. 예를 들어, 새로운 BIOS 프로그램이 있는 디지털 서명은 유효할 수 있지만, 개정 날짜는 부적절할 수 있다(즉, 현재 인스톨된 BIOS보다 더 오래된 날짜일 수 있다). 새로운 BIOS가 무효인 것으로 측정되면, 암호화 코프로세서에 의해 소거되며 결코 사용되지 않는다(단계(170)). 새로운 BIOS 프로그램이 유효하다면, 새로운 BIOS 프로그램은 동작가능하게 되며 이전의 BIOS 프로그램은 삭제된다 (단계(180)). 이 때, 시스템의 일관성을 위해 컴퓨터 시스템을 재부팅하는 것이 일반적이다.

BIOS 인증의 디지털 서명에 바탕을 둔 방법을 지원하기위해, 배포 BIOS 소프트웨어 업그레이드에 매입된 디지털 서명은 산업 협회, 또는 유사한 조직에 의해 서명 또는 승인되어야 한다. 이 협회 관계자는 자신의 BIOS 코드를 현장 업그레이드하길 원하는 BIOS 벤더이다. 이 기업의 한 가지 기능은 디지털 증명을 자신의 BIOS 벤더 멤버에게 발생시키는 것이며, 특히 BIOS 업그레이드 소프트웨어에서 사용될 디지털 증명을 각 벤더에게 할당하는 것이다. 이 협회는 BIOS 인증 프로시저동안 암호화 코프로세서에 의해 사용될 공용키를 제공한다. 암호화 코프로세서는 BIOS 벤더를 위해 산업 협회의 공용키와 함께 미리 로드될 것이며 따라서 BIOS 업그레이드 코드에 매입된 어떠한 디지털 서명도 검증할 수 있을 것이다. 대체하여, 암호화 코프로세서는 산업 협회 공용키를 얻기위해 증명 체인을 인증하기위해 사용될 수 있는 또다른 공용키와 함께 미리 로드될 수 있다. (예를 들어 코드가 역으로 처리되는 것을 방지하기위해) 필요하다면 BIOS 업그레이드 코드는 인코딩될 수 있다. 산업 협회에 의해 발생된 디지털 서명 또는 증명은 일반적으로 신용있는 BIOS 벤더의 인증을 나타내기에, (증명 또는 서명을 생성할 때 사용되는 비밀 개인키를 얻지 못한다면) 침입자는 직접 또는 간접적인 바이러스 공격으로 BIOS 코드를 파손시킬 수 없다.

(도시되지 않은) 또다른 실시예에서, 암호화 코프로세서는 호스트 프로세서의 일부이다. 호스트 프로세서는 암호화 코프로세서 및 BIOS 프로그램을 포함한다. 안전 프로세서로서 자체 동작하는 호스트 프로세서는 상기 설명된 바와같이 유사한 방식으로 BIOS 업그레이드에 대한 인증 및 유효성 검사를 수행한다. 호스트 프로세서는 BIOS 벤더를 위한 산업 협회의 공용키와 함께 미리 로드될 것이며 따라서 BIOS 갱신 코드에 매입된 어떠한 디지털 서명도 검증할 수 있을 것이다.

(도시되지 않은) 또다른 실시예에서, BIOS 프로그램은 인쇄배선 회로기판 ('PCB')에 위치하거나 시스템 확장 슬롯에 카드가 플러그인된다. 암호화 코프로세서는 동일한 PCB 카드 또는 다른 PCB 카드 또는 호스트 프로세서내에 위치할 수 있다. 시스템내에 위치하는 것에 상관없이, 암호화 코프로세서가 BIOS 프로그램에 액세스할 수 있는한, 암호화 코프로세서는 상기 설명된 바와같이 인증 및 유효성 검사를 수행할 수 있다.

본 발명이 도시된 실시예와 함께 설명되었지만, 본 설명은 제한된 것이 아니다. 본 발명의 다른 실시예뿐만 아니라 도시된 실시예의 다양한 수정이 있을 수 있다는 것은, 본 발명이 본 발명의 사상과 범위내에 있는 당 기술에 숙련된 당업자에게는 명백한 것이다.

(57) 청구의 범위

청구항 1

실행가능한 코드를 안전하게 갱신하는 시스템에 있어서,

코드 갱신을 기억하는 제 1 기억 수단;

상기 실행가능한 코드를 기억하는 제 2 기억 수단; 및

상기 제 2 기억 수단에 연결되며, 디바이스 식별에 의거하여 상기 제 1 기억 수단과 상기 코드 갱신을 인증하고 타당성 검사를 하는 제 1 처리 수단을 포함하는 것을 특징으로 하는 시스템.

청구항 2

제 1 항에 있어서, 실행가능한 코드는 기본 입출력 시스템인 것을 특징으로 하는 시스템.

청구항 3

제 1 항에 있어서, 제 1 기억 수단은 컴퓨터 네트워크에서 전자적으로 전송될 수 있는 파일 그리고 대용량 기억 디바이스중 한 개인 것을 특징으로 하는 시스템.

청구항 4

제 1 항에 있어서, 제 2 기억 수단은 수정가능한 비휘발성 메모리 디바이스인 것을 특징으로 하는 시스템.

청구항 5

제 1 항에 있어서, 제 1 처리 수단은 암호화 프로세서를 포함하는 것을 특징으로 하는 시스템.

청구항 6

제 1 항에 있어서, 제 1 처리 수단에 의해 수신된 디바이스 식별에는 디지털 서명이 포함되는 것을 특징

으로 하는 시스템.

청구항 7

제 1 항에 있어서, 상기 실행가능한 코드는 인코딩된 코드가 생성되도록 인코딩되는 것을 특징으로 하는 시스템.

청구항 8

제 1 항에 있어서, 상기 실행가능한 코드를 실행하기위해 상기 제 1 처리 수단과 통신하는 제 2 처리수단을 더 포함하는 것을 특징으로 하는 시스템.

청구항 9

제 7 항에 있어서, 상기 인코딩된 코드는 디코딩된 코드가 생성되도록 디코딩되는 것을 특징으로 하는 시스템.

청구항 10

실행가능한 코드를 안전하게 갱신하는 시스템에 있어서,

코드 갱신을 포함하는 제 1 기억 소자;

상기 실행가능한 코드를 포함하는 제 2 기억 소자; 및

디바이스 식별에 의거하여 상기 제 1 기억 소자와 상기 코드 갱신을 인증하고 타당성 검사를 하며, 상기 제 2 기억 소자에 연결된 안전 프로세서를 포함하는 것을 특징으로 하는 시스템.

청구항 11

제 10 항에 있어서, 실행가능한 코드는 기본 입출력 시스템인 것을 특징으로 하는 시스템.

청구항 12

제 10 항에 있어서, 제 1 기억 소자는 컴퓨터 네트워크에서 전자적으로 전송될 수 있는 파일 그리고 대용량 기억 디바이스중 한 개인 것을 특징으로 하는 시스템.

청구항 13

제 10 항에 있어서, 제 2 기억 소자는 수정가능한 비휘발성 메모리 디바이스인 것을 특징으로 하는 시스템.

청구항 14

제 10 항에 있어서, 안전 프로세서는 암호화 프로세서인 것을 특징으로 하는 시스템.

청구항 15

제 10 항에 있어서, 상기 안전 프로세서에 의해 수신된 디바이스 식별에는 디지털 서명이 포함되는 것을 특징으로 하는 시스템.

청구항 16

제 10 항에 있어서, 상기 실행가능한 코드는 인코딩된 코드가 생성되도록 인코딩되는 것을 특징으로 하는 시스템.

청구항 17

제 10 항에 있어서, 상기 실행가능한 코드를 실행하기위해 상기 안전 프로세서와 통신하는 호스트 프로세서를 더 포함하는 것을 특징으로 하는 시스템.

청구항 18

제 16 항에 있어서, 상기 인코딩된 코드는 디코딩된 코드가 생성되도록 디코딩되는 것을 특징으로 하는 시스템.

청구항 19

실행가능한 코드를 안전하게 갱신하는 방법에 있어서,

코드 갱신을 기억하기위해 제 1 기억 소자를 제공하는 단계;

상기 실행가능한 코드를 기억하는 제 2 기억 소자를 제공하는 단계;

디바이스 식별을 포함하기위해 상기 제 1 기억 소자를 구성하는 단계;

상기 제 2 기억 소자에 액세스하는 안전 프로세서를 제공하는 단계;

상기 안전 프로세서에 의해 상기 디바이스 식별에 의거하여 상기 제 1 기억 소자를 인증하는 단계; 및

상기 제 1 기억 소자가 인증된다면 상기 코드 갱신에 의해 상기 실행가능한 코드를 갱신하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 20

제 19 항에 있어서, 갱신하는 단계에 앞서, 제 1 기억 소자에 있는 상기 코드 갱신의 타당성을 검사하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 21

제 19 항에 있어서, 실행가능한 코드는 기본 입출력 시스템인 것을 특징으로 하는 방법.

청구항 22

제 19 항에 있어서, 제 2 기억 소자에 제공되는 상기 실행가능한 코드는 인코딩된 포맷인 것을 특징으로 하는 방법.

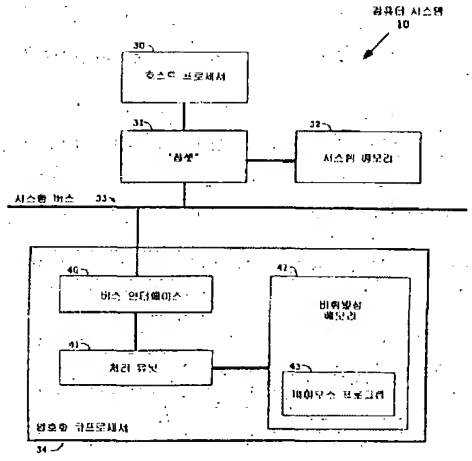
청구항 23

제 19 항에 있어서, 상기 실행가능한 코드가 실행되도록 상기 안전 프로세서와 통신하는 호스트 프로세서를 제공하는 단계를 더 포함하는 것을 특징으로 하는 방법.

요약

서브시스템은 플래시 메모리와 같은 수정가능 비휘발성 메모리에 매입된 바이오스 프로그램 코드의 미허가 수정을 방지한다. 바이오스 메모리 디바이스(42)를 포함하는 암호화 코프로세서(34)는 공개/개인 키 프로토콜에 의거하여 바이오스 업그레이드에 대한 인증 및 타당성 검사를 수행한다. 인증은 바이오스 업그레이드에 매입된 디지털 서명을 검사함으로써 수행된다.

대표도

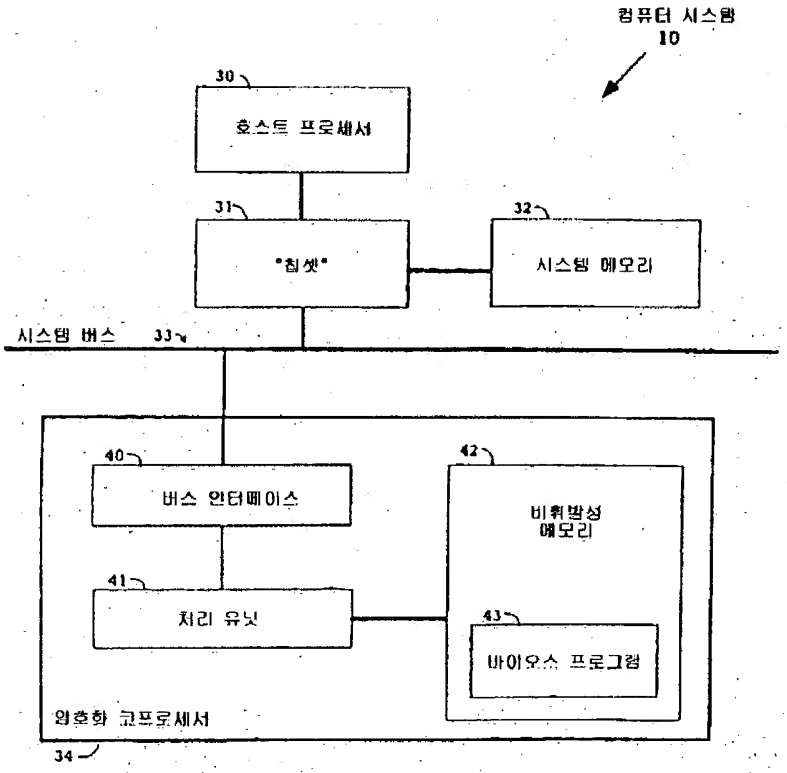


색인어

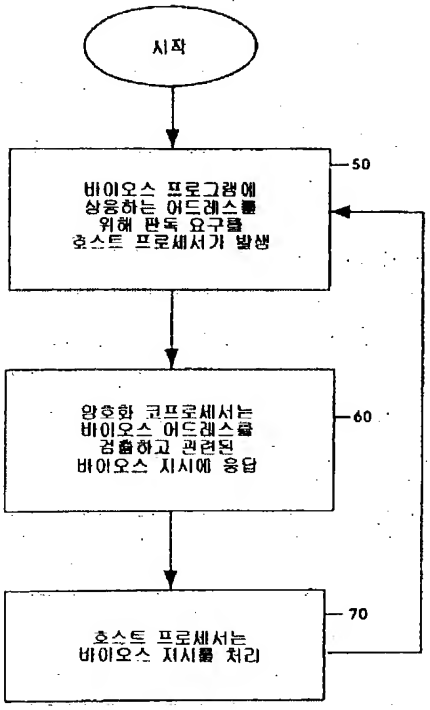
암호화 코프로세서, 디지털 서명, 인증, 안전 프로세서

도면

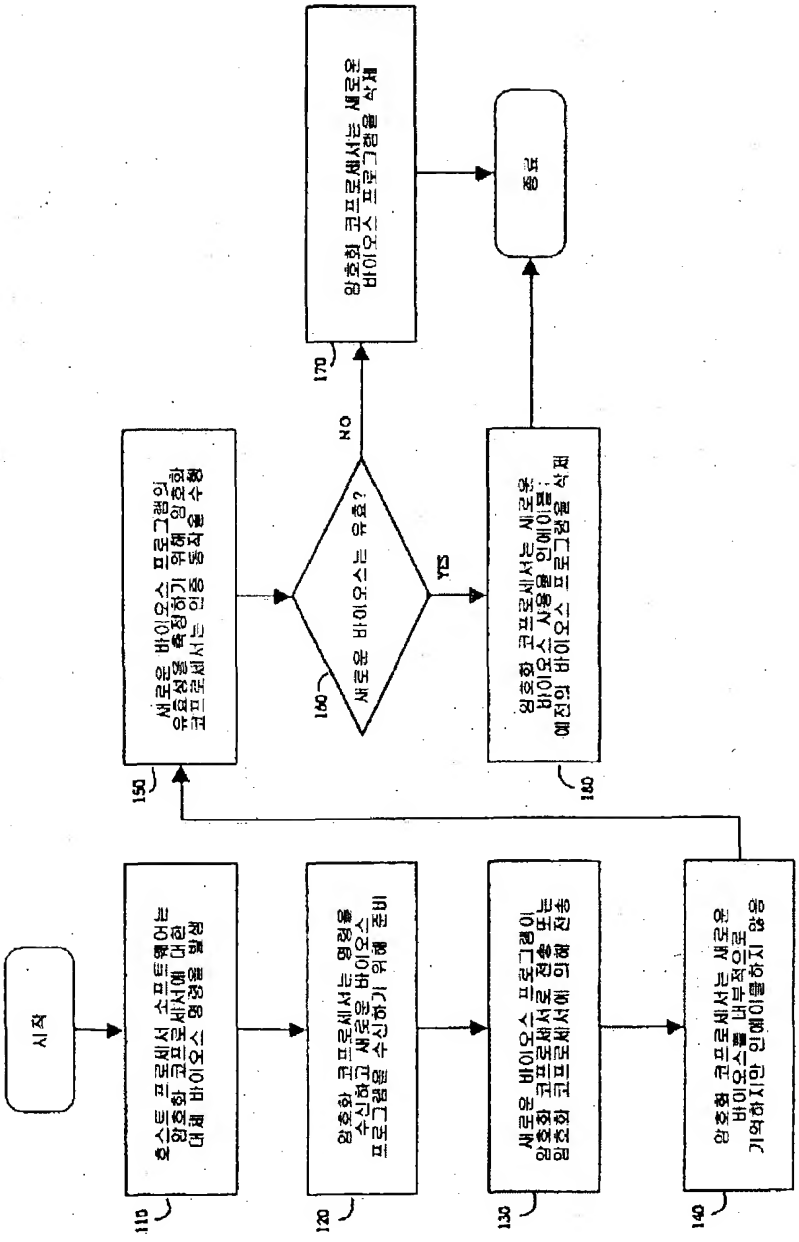
도면1


컴퓨터 시스템
10
30
호스트 프로세서
31
"칩셋"
32
시스템 메모리
시스템 버스
33
40
버스 인터페이스
42
비휘발성
메모리
41
처리 유닛
43
바이오스 프로그램
암호화 코프로세서
34

도면2


시작
바이오스 프로그램에 상응하는 어드레스를 위해 판독 요구를 호스트 프로세서가 발생
50
암호화 코프로세서는 바이오스 어드레스를 검출하고 관련된 바이오스 지시에 응답
60
호스트 프로세서는 바이오스 지시를 처리
70

도면3


시작
호스트 프로세서 소프트웨어는 암호화 코프로세서에 대한 대체 바이오스 명령을 실행
115
암호화 코프로세서는 명령을 수신하고 새로운 바이오스 프로그램을 수신하기 위해 준비
120
새로운 바이오스 프로그램이 암호화 코프로세서로 전송 또는 암호화 코프로세서에 의해 전송
130
암호화 코프로세서는 새로운 바이오스를 내부적으로 기억하지만 인에이블하지 않음
140
암호화 코프로세서는 새로운 바이오스 사용을 인에이블; 예전의 바이오스 프로그램을 삭제
160
새로운 바이오스 프로그램의 유효성을 확인하기 위해 암호화 코프로세서는 인증 동작을 수행
150
새로운 바이오스는 유효?
160
YES
NO
암호화 코프로세서는 새로운 바이오스 프로그램을 삭제
170
종료